

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA

FILED

08 FEB 19 PM 2:12

In the Matter of the Search of

7267 Camino Degrazia, Unit 22  
San Diego, California

APPLICATION AND AFFIDAVIT  
FOR SEARCH WARRANT

CLERK, U.S. DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA

DEPUTY

CASE NUMBER:

08 MJ 0484

I, Todd Walbridge, being duly sworn depose and say:

I am a Special Agent of the Federal Bureau of Investigation and have reason  
to believe that on the property or premises known as:

See Attachment A

in the Southern District of California there is now concealed a certain person  
or property, namely:

See Attachment B


which is:

**ORDERED SEALED BY COURT**

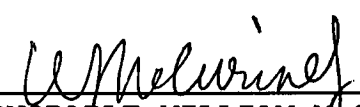
unsealed 2/25/08

Evidence, fruits of crime, property designed for use or used in committing  
criminal offenses including violations of Title 18, United States Code, Sections  
1030 and 1832. The facts to support a finding of probable cause are as follows:

See attached Affidavit of Todd Walbridge continued on the attached sheet and  
made a part hereof.   X   Yes        No

  
TODD WALBRIDGE  
Special Agent  
Federal Bureau of Investigation

Sworn to before me, and subscribed in my presence  
February 19, 2008 at San Diego, California:

  
HONORABLE WILLIAM MCCURINE, JR.  
UNITED STATES MAGISTRATE JUDGE

Attachment A

The residence of Bradley Dierking, which is located at 7267 Camino Degrazia, Unit 22, San Diego, California.

ATTACHMENT B

Authorization is sought to search for and seize evidence that Bradley Dierking accessed the computer network of Geary Interactive without authority, including the website [www.andreasroell.com](http://www.andreasroell.com), defaced the website and reservations system for Miraval Resort at [www.miravalresort.com](http://www.miravalresort.com), and accessed and copied leads from one or databases of Geary Interactive without authority in violation of Title 18, United States Code, Sections 1030 and 1832. Authorization to search includes any detached structures from the primary premises if such additional structures exist. This authorization includes the search of physical documents and includes electronic data to include deleted data, remnant data and slack space. The seizure and search of computers and computer media will be conducted in accordance with paragraph 29 of the affidavit submitted in support of this warrant. Items to be seized includes the following:

- a. All computer systems, software, peripherals and data storage devices.
- b. All temporary and permanent files and records of any kind relating to Geary Interactive, [andreasroell.com](http://andreasroell.com), Miraval Resorts, University of Phoenix and the Institute for Professional Development including but not limited to computer logs, database files and communications;
- c. All temporary and permanent files and records reflecting unauthorized access to the Geary Interactive computer network; and,
- d. All records and documents that identify the person(s) using any seized computers.

1           AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

2           I, Todd Walbridge, Special Agent of the Federal Bureau of  
3 Investigation (FBI), being duly sworn, hereby declare as follows:

4           1. I am employed as a Special Agent of the Federal Bureau of  
5 Investigation (FBI) and have been so for more than four years. I am  
6 currently assigned to the Cyber Squad in the San Diego Division. I  
7 have received training in general law enforcement and in Cyber  
8 investigations including crimes committed utilizing computers and  
9 computer networks, such as computer intrusions, denial of service  
10 attacks and malicious code. I have experience in investigations  
11 concerning Cyber crimes, white collar crimes and violent crimes within  
12 the Criminal and Cyber Divisions of the FBI. I have participated in  
13 criminal investigations involving computer intrusions, bank fraud,  
14 investment fraud, bank robberies, fugitives, innocent images and  
15 kidnappings. Prior to my employment as a Special Agent, I was  
16 employed in the computer technology field for more than eight years.

17           2. Since this affidavit is being submitted for the limited  
18 purpose of seeking authorization for a search warrant, I have not set  
19 forth every fact learned during the course of the investigation.

20           3. This affidavit is in support of an application by the United  
21 States of America for a warrant to search for evidence, fruits, and  
22 instrumentalities of violations of federal law including Title 18,  
23 United States Code, Sections 1030 (computer hacking) and 1832 (theft  
24 of trade secrets) criminal activity as described in Attachment B,  
25 located at the residence of Bradley Dierking, 7267 Camino Degrazia,  
26 Unit 22, San Diego, California 92111, as described in Attachment A.

27                   FACTS SUPPORTING PROBABLE CAUSE

28           4. Geary Interactive is an online/digital advertising agency

1 whose services include website design, online marketing, search engine  
2 marketing, e-commerce and technology solutions. Geary Interactive is  
3 based in San Diego, California. Miraval Resort is a luxury resort and  
4 spa with locations in Tucson, Arizona and in Costa Rica. Miraval  
5 Resort was one of Geary Interactive's most prestigious clients. Geary  
6 Interactive was the online advertising agency for Miraval Resort.  
7 Geary personnel designed and programmed the Miraval Resort's website  
8 (www.miravalresort.com). Geary was responsible for maintaining and  
9 updating the content on the website, to include database management  
10 of the online reservation system.

11 5. On June 7, 2007, Geary Interactive was notified by Miraval  
12 Resort of an unauthorized change made to the reservations page on  
13 Miraval Resort's website. Miraval was alerted to a change in their  
14 website by telephone calls received from their customers who were  
15 attempting to book a visit to the luxury resort and spa. The  
16 reservations page had been defaced and said, "ANDREAS ROELL IS A  
17 HOMOSEXUAL" and "LAURIE KUHN IS A STUPID FUCKING JEW." The attacker's  
18 activities caused the reservations page to be taken offline for four  
19 days. Miraval Resort also has terminated its relationship with Geary  
20 Interactive.

21 6. Geary Interactive staff were assigned to determine the  
22 circumstances of the breach of their systems and the defacement of the  
23 Miraval website. The web server log files were reviewed for any  
24 unusual external access to the servers. Under normal conditions, only  
25 Geary Interactive's IP address(es) should show up in the logs. In the  
26 logs they discovered several unknown IP addresses accessing their  
27 system around the date and time of the compromise. They searched all  
28

1 of the server logs for similar IP addresses. This search revealed the  
2 compromised areas in their network that were being accessed and used  
3 to exploit the servers' databases. The File Transfer Protocol (FTP)<sup>1/</sup>  
4 logs and Web Access Logs revealed that another domain owned and  
5 operated by Geary Interactive, andreasroell.com, was being used to  
6 deface the Miraval Resort Website. Geary Interactive discovered that  
7 the attacker was using phpMyAdmin<sup>2/</sup> to conduct malicious activity.

8 7. Geary Interactive discovered that the attacker also accessed  
9 and may have downloaded educational leads for Geary Interactive's  
10 client, University of Phoenix. These leads are purchased by the  
11 University of Phoenix at \$5 to \$100 per lead. The compromised database  
12 contained 21,678 leads. Geary Interactive explained that these leads  
13 can be sold to any educational institution. If the leads were sold  
14 at the minimum purchase price of \$5 per lead, the financial gain would  
15 be approximately \$108,390.

16 8. Other Geary Interactive clients were affected by additional  
17 malicious activity. The Institute for Professional Development (IPD)  
18 is another educational client of Geary Interactive. The IPD database,  
19 which allows IPD campuses to access and view potential student leads  
20 so that they may be contacted, was accessed and usernames and/or

---

21  
22 <sup>1/</sup>"FTP or File Transfer Protocol is used to transfer data from one computer to  
23 another over the Internet, or through a network. Specifically, FTP is a commonly  
24 used protocol for exchanging files over any TCP/IP [Internet] based network to  
25 manipulate files on another computer on that network regardless of which operating  
systems are involved (if the computers permit FTP access)." - Wikipedia  
(<http://en.wikipedia.org>)

26 <sup>2/</sup>phpMyAdmin is an open source tool written in PHP intended to handle the  
27 administration of MySQL over the Internet. Currently it can create and drop  
databases, create/drop/alter tables, delete/edit/add fields, execute any SQL  
statements, and manage keys on fields." - Wikipedia (<http://en.wikipedia.org>)

1 passwords were changed and/or deleted. This affected approximately  
2 30-40 IPD campuses. Geary Interactive was forced to reset/reassign  
3 passwords for the affected IPD campuses and then contact them with  
4 their new passwords.

5 9. Geary Interactive's ProFTPD<sup>3/</sup> logs indicated unauthorized  
6 access of their system began on May 14, 2007 and continued through  
7 June 14, 2007. These ProFTPD logs show FTP sessions originating from  
8 70.166.27.13, starting on May 14, 2007 and continuing through June 8,  
9 2007. ProFTPD logs recorded the following unauthorized access:  
10 Thirteen events on May 14, 2007; six events on May 16, 2007; and nine  
11 events on June 4, 2007.

12 10. On August 23, 2007, I performed an IP trace route using the  
13 Internet website/tool, <http://visualtracroute.visualware.com>. The  
14 results indicate that IP Address 70.166.27.13 resolves back to  
15 mail.castlead.com via Cox Communication, more specifically Castle &  
16 Associates, also known as Castle Advertising, 2470 E. Street, San  
17 Diego, California ([www.castlead.com](http://www.castlead.com)). These results were confirmed  
18 on January 3, 2007, when Cox Communication provided subpoena results  
19 indicating that the IP Address 70.166.27.13 was assigned to Castle  
20 Advertising, 2470 E Street, San Diego, California.

21 11. Bradley John Dierking is a former employee of Geary  
22 Interactive who left to take a job with Castle Advertising/EDU  
23 Interactive. Castle Advertising and Geary Interactive previously had  
24 a close business relationship. They were advertising partners in  
25 which Castle Advertising handled the traditional advertising and Geary

---

26  
27 <sup>3/</sup>"ProFTPD is an FTP server." - Wikipedia (<http://en.wikipedia.org>)

1 Interactive handled the interactive/online advertising for their  
2 shared clients. However, Castle Advertising began losing clients as  
3 the clients decreased their investments in traditional advertising  
4 and invested more money in online/interactive advertising with Geary  
5 Interactive. This resulted in the deteriorating of the Geary/Castle  
6 relationship.

7 12. Castle Advertising has employed Dierking as the Interactive  
8 Manager and Programming Director for their interactive/online  
9 advertising component named EDU Interactive. EDU Interactive was  
10 developed by Castle Advertising in response to their clients'  
11 online/interactive needs and to help them retain clients who were  
12 moving away from print and media advertising to online advertising.  
13 David Castle is listed as the Owner/Partner of EDU Interactive on  
14 their website, [www.eduinteractive.com](http://www.eduinteractive.com). EDU Interactive shares the  
15 same address as Castle Advertising and consists of many of the same  
16 staff members. A profile of Dierking appears on the EDU Interactive  
17 website. EDU Interactive's targeted clients are educational  
18 institutions.

19 13. Andreas Roell and Laurie Kuhn, the persons slandered on the  
20 Miraval Resort's website, are employees of Geary Interactive. Roell  
21 is the President and Chief Executive Officer and Kuhn is the Strategic  
22 Planning and Analytics Manager for Geary Interactive. According to  
23 both, Dierking did not get along with either Roell or Kuhn and this  
24 strife inevitably led to his resignation on April 30, 2007.

25 14. Dierking was employed by Geary Interactive as their Lead  
26 Programmer from May 15, 2005 until April 30, 2007. As the Lead  
27 Programmer, Dierking's job duties included designing and programming  
28



1 client websites and databases. He was also responsible for  
2 controlling access to the website content and to the back end  
3 databases through the assignment of usernames and passwords. He had  
4 unlimited access to all of Geary Interactive's clients' websites,  
5 databases and content contained on those websites.

6 15. On or around May 29-30, 2007, Andreas Roell (President of  
7 Geary Interactive) contacted both David Castle and Brad Dierking to  
8 inform them that Dierking was in violation of his non-compete and non-  
9 disclosure agreements that he had signed with Geary Interactive.  
10 Roell threatened legal action against Dierking. This may have been  
11 the event that precipitated the attack on Geary.

12 16. As part of its investigation of the computer intrusion,  
13 Geary Interactive utilized a program called "maos trap" to log  
14 attempted computer intrusions and possibly further identify the  
15 intruder. On June 12, 2007, Geary Interactive logged the following  
16 attempted computer intrusions:

<u>Date</u>	<u>Time</u>	<u>Username</u>	<u>Password</u>	<u>IP Address</u>
06/12/2007	16:35:40	johnm	cat\$711T	68.183.189.165
06/12/2007	16:36:29	chris	lethal55	68.183.189.165
06/12/2007	16:39:28	adloc3	Noc3lycB	72.25.103.119

21 The captured usernames and passwords were active but were old. They  
22 date from the time that Dierking set up and managed the database.  
23 Geary Interactive avoided another computer intrusion by preventing  
24 access to the phpMyAdmin application on the web server. Successfully  
25 accessing that application would open the door to the database server  
26 which contained University of Phoenix leads and Miraval Resort website  
27 content.

1        17. On or around June 14, 2007, the intruder regained access to  
2 andreasroell.com using Zend<sup>4/</sup> (andreasroell.com was the original site  
3 that was compromised and used to deface the Miraval Resort website).  
4 While employed at Geary Interactive, Dierking used the website  
5 andreasroell.com to do his testing. Zend was used to create a  
6 backdoor on the andreasroell.com site. Zend acted as a phpMyAdmin  
7 tool that allowed FTP access to the web server. Zend does not leave  
8 the traces that one would see if the intruder had used phpMyAdmin  
9 because it does not write logs like phpMyAdmin. The intruder was  
10 forced to use Zend because Geary Interactive had eliminated access to  
11 the phpMyAdmin web server after the defacement of the Miraval Resort  
12 website.

13        18. The intruder used FTP to upload his scripts used in the  
14 computer intrusion. Geary Interactive could not block FTP access  
15 because they have approximately 200-300 FTP sites that their clients  
16 need to use in order to upload content to their web sites. By using  
17 the Zend program, the intruder was able to access the databases and  
18 make changes and copy tables.

19        19. Dierking appears to be well versed in Zend, MySQL, and PHP  
20 and has posted multiple articles referencing the use of Zend on his  
21 website, www.bradino.com. A query of the Whois.net database confirmed  
22 that the website, www.bradino.com, is registered to Brad Dierking 7267  
23 Camino Degrazia, California. Under the, "About" section of  
24 www.bradino.com, there is a picture of Dierking along with text about  
25 him stating, "...I am now a PHP/MySQL Developer working full-time at

26        <sup>4/</sup> "The Zend Engine is an open source scripting engine (a Virtual Machine),  
27 commonly known for the important role in the web automation language PHP." -  
28 Wikipedia (<http://en.wikipedia.org>)

1 a leading Online Advertising Agency in Downtown San Diego."

2 20. The defacement of the Miraval website occurred on June 7,  
3 2007 and originated from IP Address 66.27.52.190. This IP address  
4 resolves back to Road Runner HoldCo, LLC, a Time Warner Cable company.  
5 On August 21, 2007, Time Warner Cable provided subpoena results  
6 indicating that the IP address 66.27.52.190 is assigned to Mission  
7 Valley Library, 2123 Fenton Parkway, San Diego, California 92108-4739.

8 21. On August 22, 2007, Ignacio Lucero, Branch Manager of the  
9 Mission Valley Branch Library, explained that the library does not  
10 monitor people's access to the library's Internet computers. There  
11 are no logs or sign up sheets to determine who used the computers.  
12 Their video surveillance is on a 24-hour loop, meaning it re-records  
13 over itself every 24-hours. The library also has an unsecured wireless  
14 network that can be accessed from the parking lot. There are no  
15 surveillance cameras covering the parking lot.

16 22. The Mission Valley Library, located at 2123 Fenton Parkway,  
17 San Diego, California, and Dierking's residence, located at 7267  
18 Camino Degrazia Unit 22, San Diego, California, are approximately 2.9  
19 miles apart according to Yahoo! Maps ([www.maps.yahoo.com](http://www.maps.yahoo.com)).

20 23. After June 8, 2007, Geary Interactive logged computer  
21 intrusions from IP Address, 72.25.103.119. ProFTPd logs show  
22 successful logins from username, zend, at IP Address 72.25.103.119.  
23 According to the ARIN database, IP Address 72.25.103.119 resolves back  
24 to DSL Extreme. On October 10, 2007, DSL Extreme provided subpoena  
25 results indicating that the IP Address 72.25.103.119 was assigned to  
26 Alesia Buchanan, P.O. Box 232, Del Mar, California, email address  
27 [help@socalfreenet.org](mailto:help@socalfreenet.org). ProFTPd logs recorded the following

28

1 unauthorized access: Seven events on June 8, 2007; fifteen events on  
2 June 12, 2007; and five events on June 13, 2007. The SoCalFreeNet.org  
3 network is an unsecured/open wireless network.

4 24. The "maos trap" described above shows two unauthorized  
5 breaches originating from IP Address, 68.183.189.165 on June 12, 2007.  
6 This IP Address also resolves back to DSL Extreme. On October 10,  
7 2007, DSL Extreme provided subpoena results indicating that the IP  
8 address 68.183.189.165 was assigned Real Equity Assets, Inc., 302  
9 Washington Street #152, San Diego, California, for Real Equity Assets,  
10 contact person Kreigan Brink. The Real Equity Assets network appears  
11 to be an unsecured/open wireless network.

12 25. Additional investigation has revealed the computer  
13 intrusions originating from IP Addresses 68.183.189.165 and  
14 72.25.103.119 occurred utilizing unsecured/open wireless networks  
15 belonging both Brink, doing business as Real Equity Assets, and  
16 Buchanan, doing business as SoCalFreeNet.org. Brink's address of 2470  
17 B Street, Unit A, San Diego, California is located in the same  
18 geographic area in which free wireless access is offered by  
19 SoCalFreeNet.org. SoCalFreeNet.org is a non-profit group that builds  
20 and deploys free public wireless networks using Wi-Fi technology.  
21 Real Equity Assets appears on SoCalFreeNet.org's website as a sponsor.

22 26. Castle Advertising/EDU Interactive (located at 2470 E  
23 Street, San Diego, California) and Real Equity Assets (located at 2470  
24 B Street, San Diego, California) are approximately 0.3 miles apart  
25 according to Yahoo! Maps ([www.maps.yahoo.com](http://www.maps.yahoo.com)).

26 27. On February 14, 2008, FBI agents surveilled Dierking leaving  
27 the offices of Castle Advertising shortly after 4:00 p.m. carrying  
28

1 what appeared to be a laptop computer bag. He placed the bag in the  
2 trunk of his car and, after a stop at a bar, drove to his home. Upon  
3 arriving, Dierking removed the laptop bag from this car and brought  
4 it into his home.

5 28. There is probable cause to believe that Dierking accessed  
6 the network of Geary Interactive repeatedly and from different  
7 locations suggesting the use of a laptop computer.

8 COMPUTER SEARCH PROTOCOL

9 29. With the approval of the court in signing this warrant,  
10 agents executing this search warrant will employ the following  
11 procedures regarding computers that may be found on the premises which  
12 may contain information subject to seizure pursuant to this warrant:

13 Forensic Imaging

14 a. There is probable cause to believe that the computer(s)  
15 used by Dierking to access Geary Interactive without authority  
16 are instrumentalities, and also may contain items that are  
17 fruits of crime - the various educational leads contained within  
18 the databases accessed without authority. Consequently, the  
19 computer is subject to seizure as provided at Rule 41(c)(2) and  
20 (c)(3), Fed.R.Crim.P., and will be seized and transported  
21 offsite for imaging. Once a verified image has been obtained and  
22 the data subjected to a preliminary review, any computers which  
23 do not appear to have been used to illegally access Geary  
24 Interactive will be returned to the owner. Images, however,  
25 will be retained for thorough examination. The imaging and  
26 preliminary review process, depending upon the number of  
27 computers seized, the volume of data contained on the computers,  
28

1 any steps taken by the owners to conceal the stolen data or use  
2 of that data and the software deployed on the computers, can  
3 take up to 30 days. It should be noted that some database  
4 programs cannot be searched by keywords without first extracting  
5 the data from the image and importing it into a new, clean  
6 compatible version of the database software on a separate,  
7 forensic computer. For computers that are retained, the owner  
8 may apply in writing to the undersigned for return of specific  
9 data which is not subject to seizure which the owner requires.  
10 The Federal Bureau of Investigation will reply in writing. In  
11 the event that the owner's request is granted, arrangements will  
12 be made for a copy of the requested data to be obtained by the  
13 owner. If the request is denied, the owner will be directed to  
14 Rule 41(g), Federal Rules of Criminal Procedure.

15 b. A forensic image is an exact physical copy of the hard  
16 drive or other media. It is essential that a forensic image be  
17 obtained prior to conducting any search of the data for  
18 information subject to seizure pursuant to this warrant. A  
19 forensic image captures all of the data on the hard drive or  
20 other media without the data being viewed and without changing  
21 the data in any way. This is in sharp contrast to what  
22 transpires when a computer running the common Windows operating  
23 system is started, if only to peruse and copy data - data is  
24 irretrievably changed and lost. Here is why: When a Windows  
25 computer is started, the operating system proceeds to write  
26 hundreds of new files about its status and operating  
27 environment. These new files may be written to places on the

1 hard drive that may contain deleted or other remnant data. That  
2 data, if overwritten, is lost permanently. In addition, every  
3 time a file is accessed, unless the access is done by trained  
4 professionals using special equipment, methods and software, the  
5 operating system will re-write the metadata for that file.  
6 Metadata is information about a file that the computer uses to  
7 manage information. If an agent merely opens a file to look at  
8 it, Windows will overwrite the metadata which previously  
9 reflected the last time the file was accessed. The lost  
10 information may be critical.

11 c. Special software, methodology and equipment is used to  
12 obtain forensic images. Among other things, forensic images  
13 normally are "hashed", that is, subjected to a mathematical  
14 algorithm to the granularity of 1038 power, an incredibly large  
15 number much more accurate than the best DNA testing available  
16 today. The resulting number, known as a "hash value" confirms  
17 that the forensic image is an exact copy of the original and  
18 also serves to protect the integrity of the image in perpetuity.  
19 Any change, no matter how small, to the forensic image will  
20 affect the hash value so that the image can no longer be  
21 verified as a true copy.

#### 22 Forensic Analysis

23 d. After obtaining a forensic image, the data will be  
24 analyzed. Analysis of the data following the creation of the  
25 forensic image is a highly technical process that requires  
26 specific expertise, equipment and software. There are literally  
27 thousands of different hardware items and software programs that



1 can be commercially purchased, installed and custom-configured  
2 on a user's computer system. Computers are easily customized by  
3 their users. Even apparently identical computers in an office  
4 environment can be significantly different with respect to  
5 configuration, including permissions and access rights,  
6 passwords, data storage and security. It is not unusual for a  
7 computer forensic examiner to have to obtain specialized  
8 hardware or software, and train with it, in order to view and  
9 analyze imaged data.

10 e. Analyzing the contents of a computer, in addition to  
11 requiring special technical skills, equipment and software also  
12 can be very tedious. It can take days to properly search a  
13 single hard drive for specific data. Searching by keywords, for  
14 example, often yields many thousands of "hits," each of which  
15 must be reviewed in its context by the examiner to determine  
16 whether the data is within the scope of the warrant. Merely  
17 finding a relevant "hit" does not end the review process. As  
18 mentioned above, the computer may have stored information about  
19 the data at issue: who created it, when it was created, when  
20 was it last accessed, when was it last modified, when was it  
21 last printed and when it was deleted. Sometimes it is possible  
22 to recover an entire document that never was saved to the hard  
23 drive if the document was printed. Operation of the computer by  
24 non-forensic technicians effectively destroys this and other  
25 trace evidence. Moreover, certain file formats do not lend  
26 themselves to keyword searches. Keywords search text. Many  
27 common electronic mail, database and spreadsheet applications do



1 not store data as searchable text. The data is saved in a  
2 proprietary non-text format. Microsoft Outlook data is an  
3 example of a commonly used program which stores data in a non-  
4 textual, proprietary manner- ordinary keyword searches will not  
5 reach this data. Documents printed by the computer, even if the  
6 document never was saved to the hard drive, are recoverable by  
7 forensic examiners but not discoverable by keyword searches  
8 because the printed document is stored by the computer as a  
9 graphic image and not as text. Similarly, faxes sent to the  
10 computer are stored as graphic images and not as text.


11 f. Analyzing data on-site has become increasingly  
12 impossible as the volume of data stored on a typical computer  
13 system has become mind-boggling. For example, a single megabyte  
14 of storage space is the equivalent of 500 double-spaced pages of  
15 text. A single gigabyte of storage space, or 1,000 megabytes,  
16 is the equivalent of 500,000 double-spaced pages of text.  
17 Computer hard drives are now capable of storing more than 100  
18 gigabytes of data and are commonplace in new desktop computers.  
19 And, this data may be stored in a variety of formats or  
20 encrypted. The sheer volume of data also has extended the time  
21 that it takes to analyze data in a laboratory. Running keyword  
22 searches takes longer and results in more hits that must be  
23 individually examined for relevance. Even perusing file  
24 structures can be laborious if the user is well-organized.  
25 Producing only a directory listing of a home computer can result  
26 in thousands of pages of printed material most of which likely  
27 will be of limited probative value.

1 g. Based on the foregoing, searching any computer or  
2 forensic image for the information subject to seizure pursuant  
3 to this warrant may require a range of data analysis techniques  
4 and may take weeks or even months. Keywords need to be  
5 modified continuously based upon the results obtained; criminals  
6 can mislabel and hide files and directories, use codes to avoid  
7 using keywords, encrypt files, deliberately misspell certain  
8 words, delete files and take other steps to defeat law  
9 enforcement. In light of these difficulties, your affiant  
10 requests permission to use whatever data analysis techniques  
11 reasonably appear necessary to locate and retrieve digital  
12 evidence within the scope of this warrant.


13 h. All forensic analysis of the imaged data will be  
14 directed exclusively to the identification and seizure of  
15 information within the scope of this warrant.

16 **REQUEST FOR SEALING**

17 30. Premature disclosure of the search warrant, this affidavit,  
18 andr this application and the attachments thereto may jeopardize the  
19 progress of the investigation by resulting in the destruction of  
20 volatile electronic data. Consequently, we request that the search  
21 warrant and related materials be sealed until further Order of the  
22 Court.

23   
Todd Walbridge, Special Agent  
Federal Bureau of Investigation

24  
25 Subscribed and sworn to before me this  
19<sup>th</sup> day of February, 2008:

26   
27 HONORABLE WILLIAM MCCURINE, JR.  
28 UNITED STATES MAGISTRATE JUDGE